UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/089,941	09/15/2003	Bruno Dutertre	SRI/4283-2	1672

52197 7590 11/29/2006

PATTERSON & SHERIDAN, LLP
SRI INTERNATIONAL
595 SHREWSBURY AVENUE
SUITE 100
SHREWSBURY, NJ 07702

EXAMINER	
LEMMA, SAMSON B	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 11/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/089,941	DUTERTRE ET AL.	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 September 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on September 05, 2006. All independent claims, namely claims, **1, 13, 16 and 18** are amended. No claim is canceled. Thus, **claims 1-18** are pending.

Response to Arguments

2. Applicant's remark/arguments filed on regarding September 05, 2006 regarding claims 1-18 have been fully considered but are moot in view of new grounds of rejection.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1, 12-14,16-18** are rejected under 35 U.S.C. 102(e) as being unpatentable by **Tuomas Aura .** (hereinafter referred as **Aura**) (U.S. Patent No: 6, 711, 400 B1) in view of C.R. Snow (hereinafter referred as **Snow)**, article written with the title, "Simple Authentication" (Published 1994) (Reference U)

5. **As per claims 1, 13-14, 16-18 Aura discloses** a secure method of transmitting a message between a sender node [figure 4, reference HLR/AUC; authentication station] and a recipient node [figure 4, reference 407; Mobile station] within a network collaboration group, the sender and the recipient sharing a secret encryption key [Ki] **(ki, used in the function Hi meets the recitation of the encryption key which is shared at both authentication center and mobile station)** and an expected nonce value [RAND1] **(the nonce value as described in the disclosure is just a number so RAND1 or random number meets the recitation of the expected nonce value)** comprising:

Generating a new nonce value [RAND 2] known to the sender [Figure 4, reference 404; RAND2] (**The authentication center generate a new nonce value RAND2 at the authentication center/sender**)

Encrypting the message including the expected nonce value and the new nonce value, using the encryption key[See figure 4, reference 405 and H1] (**Both the new nonce value RAND 2 which is generated at the sending station, the expected nonce value RAND1 are encrypted by the key Ki using the hash function H1**];

Transmitting the encrypted message [SRES1] **from the sender** [Figure 4, reference 405] **to the recipient** node [Figure 4, reference 407]; and

Furthermore, **Aura discloses,** verifying, by the recipient, that the encrypted message[SRES1] includes the expected nonce value[figure 4, reference "408"] (**If the encrypted message SRES1 sent from the sender side 405 to the recipient side 407 does not include the corrected expected nonce value RAND1 then the verification test at figure 4, reference 408 fails Since SRES1' will not be equal to SRES1 otherwise it will passé the verification test**).

Aura further teaches, **wherein the expected nonce value and the new nonce value are recoverable from encrypted message using knowledge possessed by the recipient node prior to receipt of the encrypted message**. [See the "ki", shown on Figure 4, ref. Num "405" and "407"](The key "Ki", which is shown on figure 4, ref, "405" and ref. Num "407" is a knowledge possessed by the recipient node prior to the receipt of the encrypted message and the expected nonce value RAND1 and the **new nonce value RAND 2** are recoverable from the encrypted message SRES1, using "ki"/the knowledge possessed by the recipient node prior to receipt of the encrypted message)

Aura does not explicitly disclose

Wherein the encrypted message may be verified by the recipient by decrypting the encrypted message and confirming that the encrypted message includes the expected nonce value.

However, in the same field of endeavor, **Snow,** discloses the method wherein encrypted message may be verified by the recipient by decrypting the encrypted message and confirming that the encrypted message includes the expected nonce value. [See page 444, 3rd paragraph]. On page 444, 3rd paragraph the following has been disclosed. "On receipt of the 'set key' message, the workstation asks the user to supply the authorizing password, i.e. the old password corresponding to the name, and then to supply the new password. **The old password is used to create the encryption key, and the new password is used to create the new key. The nonce and the new key are then encrypted with the old key, and sent back to the host. If the nonce is succesfully decrypted, t**he database entry corresponding to <name> is updated with the new key."

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features verifying by the recipient by decrypting the encrypted message and confirming that the encrypted message includes the expected nonce value **as per teachings of Snow** into the method as taught by **Aura,** in order to provide strong authentication mechanism.

6. **As per claim 12** the combination of **Aura and Snow discloses** a secure method of transmitting a message between a sender node and a recipient node as applied to claims above. Furthermore **Aura d**iscloses the method further including receiving a copy of a prior message being transmitted as a replay attack, and rejecting the replay as illicit at least in part because

the replay does not contain the current expected nonce value. [figure 4, 408, discard connection]

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 2-11 and 15** are rejected under 35 U.S.C. 102(e) as being unpatentable by **Tuomas Aura .** (hereinafter referred as **Aura**) (U.S. Patent No: 6, 711, 400 B1) in view of C.R. Snow (hereinafter referred as **Snow)**, article written with the title, "Simple Authentication" (Published 1994) (Reference U), further in view of **Janson et al** (hereinafter referred as **Janson**) (U. S. Patent No. 5, 729, 608) (Provided with IDS)

9. **As per claims 2-3 Aura discloses** a secure method of transmitting a message between a sender node [figure 4, reference HLR/AUC; authentication station] and a recipient node [figure 4, reference 407; Mobile station] within a network collaboration group, the sender and the recipient sharing a secret encryption key [Ki] **(ki, used in the function Hi meets the recitation of the encryption key which is shared at both authentication center and mobile station**) and an expected nonce value [RAND1] **(the nonce value as described in the disclosure is just a number so RAND1 or random number meets the recitation of the expected nonce value**) comprising:

> Generating a new nonce value [RAND 2] known to the sender [Figure 4, reference 404; RAND2] **(The authentication center generate a new nonce value RAND2 at the authentication center/sender**)

Encrypting the message including the expected nonce value and the new nonce value, using the encryption key[See figure 4, reference 405 and H1] (**Both the new nonce value RAND 2 which is generated at the sending station, the expected nonce value RAND1 are encrypted by the key Ki using the hash function H1**];

Transmitting the encrypted message [SRES1] **from the sender** [Figure 4, reference 405] **to the recipient** node [Figure 4, reference 407]; and

Furthermore, **Aura discloses,** verifying, by the recipient, that the encrypted message[SRES1] includes the expected nonce value[figure 4, reference "408"] (**If the encrypted message SRES1 sent from the sender side 405 to the recipient side 407 does not include the corrected expected nonce value RAND1 then the verification test at figure 4, reference 408 fails Since SRES1' will not be equal to SRES1 otherwise it will passé the verification test**).

Aura further teaches, **wherein the expected nonce value and the new nonce value are recoverable from encrypted message using knowledge possessed by the recipient node prior to receipt of the encrypted message**. [See the "ki", shown on Figure 4, ref. Num "405" and "407"](The key "Ki", which is shown on figure 4, ref, "405" and ref. Num "407" is a knowledge possessed by the recipient node prior to the receipt of the encrypted message and the expected nonce value RAND1 and the **new nonce value RAND 2** are recoverable from the encrypted message SRES1, using "ki"/the knowledge possessed by the recipient node prior to receipt of the encrypted message)

Aura does not explicitly disclose

Wherein the encrypted message may be verified by the recipient by decrypting the encrypted message and confirming that the encrypted message includes the expected nonce value.

However, in the same field of endeavor, **Snow,** discloses the method wherein encrypted message may be verified by the recipient by decrypting the encrypted message and confirming that the encrypted message includes the expected nonce value. [See page 444, 3rd paragraph]. On page 444, 3rd paragraph the following has been disclosed. "On receipt of the 'set key' message, the workstation asks the user to supply the authorizing password, i.e. the old password corresponding to the name, and then to supply the new password. **The old password is used to create the encryption key, and the new password is used to create the new key. The nonce and the new key are then encrypted with the old key, and sent back to the host. If the nonce is succesfully decrypted, t**he database entry corresponding to <name> is updated with the new key."

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features verifying by the recipient by decrypting the encrypted message and confirming that the encrypted message includes the expected nonce value **as per teachings of Snow** into the method as taught by **Aura,** in order to provide strong authentication mechanism.

- The combination of **Aura and Snow** does not explicitly disclose

Generating a second new nonce value, known to the recipient node; transmitting a secure response from the recipient to the sender by repeating the method of claim 1, but this time using the second new nonce value in place of the new nonce value and using the new nonce value in place of the expected nonce value.

However, in the field of endeavor **Janson** discloses

Generating a second new nonce value, known to the recipient node; transmitting a secure response from the recipient to the sender by repeating the method of claim 1, but this time using the second new nonce value in place of the new nonce value and using the new nonce value in place of the expected nonce value. [figure 2, 202]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to add the features having the recipient providing the authentication information to the sender as per teachings of Janson in to the method as taught by the combination of **Aura and Snow,** in order to provide a secure communication.[See Janson, column 2, lines 9-11]

10. **As per claims 4-6 and 15** the combination of **Aura, Snow and Janson discloses** a secure method of transmitting a message between a sender node and a recipient node as applied to claims above. Furthermore **Janson** discloses the method wherein the sender is a key managing master node and the recipient is a member node of the collaboration group. [column 3,lines 30-42]

11. **As per claims 7-11 the** combination of **Aura, Snow and Janson discloses** a secure method of transmitting a message between a sender node and a recipient node as applied to claims above. Furthermore **Janson** discloses the method wherein the method is used with a key-managing master node in order to perform an authentication process for opening a collaboration group session with a new member node. [Column 3, lines 35-37; column 1, lines 41-51; column 4, lines 6-21]

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KAMBIZ ZAND
PRIMARY EXAMINER

SAMSON LEMMA
S.L.
11/18/2006
AU2132